

A Class of Two-Weight and Three-Weight Linear Codes and Their Duals

Li Liu, Xianhong Xie and Lanqiang Li

Abstract—The objective of this paper is to construct a class of linear codes with two nonzero weights and three nonzero weights by using the general trace functions, which weight distributions has been determined. These linear codes contain some optimal codes, which meets certain bound on linear codes. The dual codes are also studied and proved to be optimal or almost optimal. These codes may have applications in authentication codes, secret sharing schemes and strongly regular graphs.

Index Terms—Linear codes, Weight distribution, Dual codes, Secret sharing schemes, Authentication codes.

I. INTRODUCTION

THROUGH this paper, let p be prime and $q = p^s$, where s is a positive integer. An $[n, k, d]$ code C over F_p is a k -dimension subspace of F_p^n with minimum Hamming distance d . Let A_i denote the number of codewords with Hamming weight i in C , then $(1, A_1, \dots, A_n)$ is called the weight distribution of C .

Griesmer Bound is a generalization of the Singleton Bound and is different from other upper bounds. This one only applies to linear codes. Therefore, Griesmer Bound is presented in the following lemma[11].

Lemma 1.1. Let C be an $[n, k, d]$ code over F_q , with $k \geq 1$. Then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

The Griesmer Bound gives a lower bound on the length of a code over F_q with a specified dimension k and minimum distance d . An $[n, k, d]$ code C is called optimal if parameters $[n, k, d]$ meet this bound. An $[n, k, d]$ code C is called almost optimal if $[n, k, d+1]$ meet this bound.

Let $D = \{d_1, d_2, \dots, d_n\} \subseteq F_q^*$, then a linear code over F_p of length n is

$$C_D = \{(Tr_1^s(\beta d_1), Tr_1^s(\beta d_2), \dots, Tr_1^s(\beta d_n))\},$$

where Tr_1^s is the trace function from F_q onto F_p . D is called defining set of this code C_D . The selection of D directly affects the constructed linear codes. So we can obtain linear codes with few weights by the proper selection of D [5],[12],[13],[15],[17]. In addition, from the another view of D , let $D = \{x \in F_q : Tr_1^s(f(x)) = 0\}$ and $f(x) \in F_q(x)$. The previous work focused on changing the function $f(x)$ or generalizing the defining set of D , i.e., $f(x) = x^{2^h+1}$ [3], $f(x) = x^{\frac{q-1}{r}}(3|n)$ [9]. Ding and Ding[4] gave the weight distributions of C_D for the case $f(x) = x^2$ and proposed an open problem on calculating the weight distributions of C_D for general planar functions. Zhou et al.[7] solved this

TABLE I
THE WEIGHT DISTRIBUTION OF THE CODE OF THEOREM 2.1

Weight w	Multiplicity A_w
$p^{2m-e} - p^{2m-e-1}$	$p^{2m-e} - (p^e - 1)p^{m-e} - 1$
$(p^{2m-e-1} - p^{m-1})(p-1)$	$(p^e - 1)(q + p^m)/p^e$

problem by the quadratic bent functions. Tang et al.[10] also settled the problem by the weakly quadratic bent functions. A class of two-weight and three-weight linear codes with the general trace functions has given by Tang et al.[6]. Carlet and Ding[1] presented the minimum distance of C and C^\perp for the case $f(x) = \alpha x^{p^k+1} + \beta x$. For the case of $\frac{s}{gcd(s,k)}$ being odd, Yuan et al.[2] gave the weight distributions. However, the problem of constructing weight distributions for $\frac{s}{gcd(s,k)}$ being even is underdeveloped.

In this paper, motivated by the research work in [1] and [3], we use the more general method to construct linear codes with two and three weights. New parameters and weight distributions of such codes are determined. Some of the linear codes in this paper are optimal. Besides, linear codes with three-weight and two-weight of this paper may have applications in secret sharing schemes [16] and authentication codes [15].

II. LINEAR CODES WITH TWO WEIGHTS AND THREE WEIGHTS

In this section, we only describe the linear codes and introduce their parameters by two theorems. The proofs of their parameters will be presented later.

Let $s = 2m$, $m = et$ and $q = p^{2m}$, where m , t and e are positive integers. Define

$$D_1 = \{x \in F_q^* : Tr_e^s(x^{p^m+1}) = 0\},$$

where $Tr_e^s(x) = \sum_{i=0}^{\frac{s}{e}-1} x^{p^{ei}}$ is the general trace function. Let $D_1 = \{d_1, d_2, \dots, d_{n_1}\}$ and $n_1 = |D_1|$, we have the linear code

$$C_{D_1} = \{c_\beta : \beta \in F_q\} \quad (1)$$

where $c_\beta = (Tr_1^s(\beta d_1), Tr_1^s(\beta d_2), \dots, Tr_1^s(\beta d_{n_1}))$.

Theorem 2.1. Let $s = 2m$, $e|m$ and $e < m$. The code C_{D_1} defined in Equation (1) is a two-weight linear code with parameters $[p^{2m-e} + p^{m-e} - p^{m-1}, 2m, (p^{2m-e-1} - p^{m-1})(p-1)]$, whose weight distribution is listed in **Table I**.

Example 2.1. Let $(m, e) = (2, 1)$ and $p = 3$. Then the code C_{D_1} has parameters $[20, 4, 12]$ and weight enumerator

TABLE II

THE WEIGHT DISTRIBUTION OF THE CODE OF COROLLARY 2.2

Weight w	Multiplicity A_w
p^{2m-e-1}	$p^{2m-e} - (p^e - 1)p^{m-e} - 1$
$p^{2m-e-1} - p^{m-1}$	$(p^e - 1)(q + p^m)/p^e$

$1 + 20x^{18} + 60x^{12}$. This code is optimal due to the Griesmer bound since the optimal linear code over F_3 with length 20 and dimension 4 has minimum weight 12.

Example 2.2. Let $(m, e) = (2, 1)$ and $p = 5$. Then the code C_{D_1} has parameters $[104, 4, 80]$ and is almost optimal, while the optimal linear code has parameters $[104, 4, 81]$.

It is observed that the weights in the code C_{D_1} have a common divisor $p - 1$. This indicates that the code C_{D_1} may be punctured into a shorter one whose weight distribution can be derived from that of the original code C_{D_1} . This will be done as follows.

Note that for any $a \in F_p^*$, $Tr_e^s((ax)^{p^m+1}) = a^2 Tr_e^s(x^{p^m+1})$. We can select a subset $\overline{D_1}$ of D_1 such that

$$D_1 = (F_p^*)\overline{D_1} = \{ab : a \in F_p^*, b \in \overline{D_1}\}, \quad (2)$$

where $\frac{b_i}{b_j} \notin F_p^*$ for every pair of distinct elements $(b_i, b_j) \in \overline{D_1}^2$. Hence, the parameters and weight distributions of the $C_{\overline{D_1}}$ are given in the following corollary.

Corollary 2.2. Let $s = 2m$, $e|m$ and $e < m$. Let $\overline{D_1}$ be defined in (2). Then the code $C_{\overline{D_1}}$ is a two-weight linear code with parameters $[\frac{p^{2m-e} + p^{m-e} - p^m - 1}{p-1}, 2m, p^{2m-e-1} - p^{m-1}]$ whose weight distribution is listed in **Table II**.

Example 2.3. Let $(m, e) = (3, 1)$ and $p = 3$. the code C_{D_1} has parameters $[224, 6, 144]$. Note that the code constructed is not optimal, since an optimal $[224, 6]$ code has minimum weight 147. The code $C_{\overline{D_1}}$ has parameters $[112, 6, 72]$. This code is optimal due to the Griesmer bound since the optimal linear code with length 112 and dimension 6 has minimum weight 72.

Example 2.4. Let $(m, e) = (2, 1)$ and $p = 5$. Then the code C_{D_1} has parameters $[104, 4, 80]$ and is almost optimal. But the code $C_{\overline{D_1}}$ has parameters $[26, 4, 20]$. This code is optimal.

Define $D_2 = F_q^*$, let $D_2 = \{d_1, d_2, \dots, d_{n_2}\}$, where $n_2 = p^{2m} - 1$. We define a linear code of length n_2 over F_p by

$$C_{D_2} = \{c_{(\beta, \gamma)} : \beta \in F_q, \gamma \in F_{p^m}\}, \quad (3)$$

where

$$c_{(\beta, \gamma)} = ((Tr_1^s(\beta d_1) + Tr_1^m(\gamma d_1^{p^m+1})), (Tr_1^s(\beta d_2) + Tr_1^m(\gamma d_2^{p^m+1})), \dots, (Tr_1^s(\beta d_{n_2}) + Tr_1^m(\gamma d_{n_2}^{p^m+1}))).$$

Theorem 2.3. Let $s = 2m$. Then the code C_{D_2} defined in (3) is a three-weight linear code with parameters $[p^{2m} - 1, 3m]$ whose weight distribution is listed in **Table III**.

Example 2.5. Let $p = 5$ and $m = 1$, the code C_{D_2} has parameters $[24, 3, 19]$ and weight enumerator $1 + 24x^{20} + 96x^{19} + 4x^{24}$. This code is optimal.

Example 2.6. Let $p = 3$ and $m = 2$, the code C_{D_2} has parameters $[80, 6, 51]$ and weight enumerator $1 + 480x^{51} + 168x^{60} + 80x^{54}$. This code is optimal.

TABLE III

THE WEIGHT DISTRIBUTION OF THE CODE OF THEOREM 2.3

Weight w	Multiplicity A_w
$p^{2m-1}(p-1)$	$p^{2m} - 1$
$(p^{2m-1} + p^{m-1})(p-1)$	$p^{m-1}(p^m - 1)(p^m - p + 1)$
$p^{2m-1}(p-1) - p^{m-1}$	$(p^m - 1)(p-1)(p^{2m} - 1)$

III. PROOFS OF THE MAIN RESULTS

Our task are to prove Theorem 2.1 and 2.3. Before doing this, we need to define a constant as follows. Let

$$n_1 = |\{x \in F_q^* : Tr_e^s(x^{p^m+1}) = 0\}|, \quad (4)$$

where $Tr_e^s(x)$ is the general trace function. To prove Theorem 2.1 and 2.3, we also define the following parameter

$$N_\beta = |\{x \in F_q^* : Tr_e^s(x^{p^m+1}) = 0, Tr_1^s(\beta x) = 0\}|,$$

where $\beta \in F_q^*$. By definition and the basic facts of additive characters, for any $\beta \in F_q^*$, we have

$$\begin{aligned} N_\beta &= \frac{1}{p^{e+1}} \sum_{x \in F_q^*} \left(\sum_{\lambda \in F_{p^e}} \zeta_p^{Tr_1^s(\lambda x^{p^m+1})} \right) \left(\sum_{y \in F_p} \zeta_p^{Tr_1^s(y\beta x)} \right) \\ &= \frac{1}{p^{e+1}} \left(q + \sum_{x \in F_q} \sum_{\lambda \in F_{p^e}} \zeta_p^{Tr_1^s(\lambda x^{p^m+1})} + \sum_{\lambda \in F_{p^e}} \sum_{y \in F_p} \sum_{x \in F_q} \zeta_p^{Tr_1^s(\lambda x^{p^m+1}) + Tr_1^s(y\beta x)} \right) - 1. \end{aligned} \quad (5)$$

$$\text{Let } A = \sum_{x \in F_q} \left(\sum_{\lambda \in F_{p^e}} \zeta_p^{Tr_1^s(\lambda x^{p^m+1})} \right) \text{ and } B = \sum_{\lambda \in F_{p^e}} \sum_{y \in F_p} \sum_{x \in F_q} \zeta_p^{Tr_1^s(\lambda x^{p^m+1}) + Tr_1^s(y\beta x)}.$$

Thus, we have the following lemmas.

Lemma 3.1. Let $s = 2m$, $m = et$, $\lambda \in F_{p^e}^*$ and $\beta \in F_q$. Then

$$\sum_{x \in F_q} \zeta_p^{Tr_1^m(\lambda x^{p^m+1}) + Tr_1^s(\beta x)} = -p^m \zeta_p^{Tr_1^m(-\lambda^{-1}\beta^{p^m+1})}.$$

Proof. By the basic facts of trace functions[18, Corollary 4], we have

$$\begin{aligned} \sum_{x \in F_q} \zeta_p^{Tr_1^m(\lambda x^{p^m+1}) + Tr_1^s(\beta x)} &= \sum_{x \in F_q} \zeta_p^{Tr_1^m(\lambda x^{p^m+1} + \beta^{p^m} x^{p^m} + \beta x)} \\ &= \sum_{x \in F_q} \zeta_p^{Tr_1^m(\lambda(x+\delta)^{p^m+1} - \lambda\delta^{p^m+1})} = \zeta_p^{Tr_1^m(-\lambda\delta^{p^m+1})} ((p^m+1)) \\ &\quad \sum_{z \in F_{p^m}} \zeta_p^{Tr_1^m(\lambda z)} + 1 = -p^m \zeta_p^{Tr_1^m(-\lambda\delta^{p^m+1})}, \end{aligned}$$

where $\beta = \lambda\delta^{p^m}$ (thus $\delta^{p^m+1} = \frac{\beta^{p^m+1}}{\lambda^2}$). So this completes the proof of this Lemma. \square

Lemma 3.2. Let $s = 2m$ and $e|m$. Then $A = \sum_{\lambda \in F_{p^e}^*} \sum_{x \in F_q} \zeta_p^{Tr_1^s(\lambda x^{p^m+1})} = -(p^e - 1)p^m$ and the length n of the C_{D_1} is $p^{2m-e} - (p^e - 1)p^{m-e} - 1$.

Proof. According to Lemma 3.1, we could easily obtain the following result.

$$\begin{aligned} A &= \sum_{\lambda \in F_p^*} \sum_{x \in F_q} Tr_1^s(\lambda x^{p^m+1}) \\ &= \sum_{\lambda \in F_p^*} \left(\sum_{z \in F_p^*} (p^m + 1) \zeta_p^{Tr_1^m(\lambda z)} + 1 \right) \\ &= -(p^e - 1)p^m. \end{aligned}$$

Combining (4) and the above result, we have the length $n = \frac{1}{p^e}(q + A) - 1 = p^{2m-e} - (p^e - 1)p^{m-e} - 1$. \square

Lemma 3.3. Let $s = 2m$, $m = et$, then

$$B = \begin{cases} -(p-1)(p^e-1)p^m, & \text{if } Tr_e^m(\beta^{p^m+1}) = 0, \\ (p-1)p^m, & \text{if } Tr_e^m(\beta^{p^m+1}) \neq 0. \end{cases}$$

Proof. From the map $x \rightarrow \frac{y}{\lambda}x$ and $\lambda \rightarrow \frac{y^2}{\lambda}$, we have

$$B = \sum_{y \in F_p^*} \sum_{\lambda \in F_p^*} \sum_{x \in F_q} \zeta_p^{Tr_1^s(\lambda(x^{p^m+1} + \beta x))}.$$

By Lemma 3.1, we have

$$\begin{aligned} B &= -p^m(p-1) \sum_{\lambda \in F_p^*} \zeta_p^{Tr_1^e(\lambda Tr_e^m(\beta^{p^m+1}))} \\ &= \begin{cases} -(p-1)(p^e-1)p^m, & \text{if } Tr_e^m(\beta^{p^m+1}) = 0, \\ (p-1)p^m, & \text{if } Tr_e^m(\beta^{p^m+1}) \neq 0. \end{cases} \quad \square \end{aligned}$$

The Proof of Theorem 2.1

According to Lemma 3.2, the length of a codeword in C_{D_1} is

$$n_1 = p^{2m-e} - (p^e - 1)p^{m-e} - 1.$$

It follows from (5), Lemma 3.2 and Lemma 3.3 that we have

$$wt(c_\beta) \in \{p^{2m-e} - p^{2m-e-1}, (p^{2m-e-1} - p^{m-1})(p-1)\},$$

and the code C_{D_1} has all the two weights in the set above.

Define $w_1 = p^{2m-e} - p^{2m-e-1}$, $w_2 = (p^{2m-e-1} - p^{m-1})(p-1)$. By Lemma 3.2, we have

$$\begin{aligned} A_{w_1} &= p^{2m-e} - (p^e - 1)p^{m-e} - 1, \\ A_{w_2} &= (p^e - 1)(q + p^m)/p^e. \end{aligned}$$

The Proof of Theorem 2.3

Combining (3), Lemma 3.1 and Lemma 3.3, we obtain the following results.

$$wt(c_{(\gamma, \beta)}) = q - p^{-1} \sum_{y \in F_p} \sum_{x \in F_q} \zeta_p^{y(Tr_1^m(\gamma x^{p^m+1}) + Tr_1^s(\beta x))}$$

$$= \begin{cases} p^{2m-1}(p-1), & \text{if } \gamma = 0, \beta \neq 0, \\ (p^{2m-1} + p^{m-1})(p-1), & \text{if } Tr_1^m(\gamma^{-1}\beta^{p^m+1}) = 0, \\ p^{2m-1}(p-1) - p^{m-1}, & \text{if } Tr_1^m(\gamma^{-1}\beta^{p^m+1}) \neq 0. \end{cases}$$

Let $w_1 = p^{2m-1}(p-1)$, $w_2 = (p^{2m-1} + p^{m-1})(p-1)$, $w_3 = p^{2m-1}(p-1) - p^{m-1}$. We determine the number A_{w_i} of codewords with weight w_i in C_{D_2} . It is possible to prove the minimum weight of the dual code $C_{D_2}^\perp$ is at least 3. Therefore,

the first three Pless Power Moment lead to the following system of equations:

$$\begin{cases} A_{w_1} + A_{w_2} + A_{w_3} = p^{3m} - 1, \\ w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} = p^{3m-1} n_2 (p-1), \\ w_1^2 A_{w_1} + w_2^2 A_{w_2} + w_3^2 A_{w_3} = p^{3m-2} n_2 (p-1) (n_2 p - n_2 + 1), \end{cases}$$

where $n_2 = p^{2m} - 1$. Solving the system of equations yields the weight distribution in **Table III**. \square

IV. THE DUALS OF THE CODES C_{D_1} AND C_{D_2}

In this section, for the duals $C_{D_1}^\perp$ and $C_{D_2}^\perp$, we have the following two theorems.

Theorem 4.1. Let d_1^\perp denote the minimum distance of the $C_{D_1}^\perp$. The definition of C_{D_1} can be found in Theorem 2.1. Then $2 \leq d_1^\perp \leq 4$, $d_1^\perp = 3$ if $p = 2$ and $m \geq 3$.

Proof. Clearly, D_1 does not contain the zero element of F_q , the minimum distance of $C_{D_1}^\perp$ cannot be one. Besides, d_1^\perp is at most 4 due to the Sphere Packing Bound. Hence, we have $2 \leq d_1^\perp \leq 4$.

If $p = 2$, the minimum distance $C_{D_1}^\perp$ cannot be 2, Since D_1 is not a multiset, any two elements d_i and d_j of D_1 must be distinct if $i \neq j$.

$D_1 = \{x \in F_q^* : Tr_e^s(x^{p^m+1}) = 0\}$. Obviously, $F_{p^e}^* \subset D_1$. For any two distinct elements $a, b \in F_{p^e}^* \subset D_1$, we have $a + b \in F_{p^e}^* \subset D_1$. Besides, if $m \geq 3$, we have $2^{2m-e} + 2^{m-e} - 2^m \geq 2m - 2$. Hence, the minimum distance of $C_{D_1}^\perp$ is 3. \square

Example 4.1. Let $(m, e) = (2, 1)$ and $p = 3$. Then the code $C_{D_1}^\perp$ has parameters $[20, 16, 3]$ and is optimal.

Example 4.2. Let $p = 2$, $m = 3$ and $e = 1$. Then the code $C_{D_1}^\perp$ has parameters $[27, 21, 3]$ and is almost optimal. This code is optimal due to the Griesmer bound since the optimal linear code with length 27 and dimension 21 has minimum weight 4.

Theorem 4.2. Let d_2^\perp denote the minimum distance of the $C_{D_2}^\perp$. The code of C_{D_2} is defined in equation (3). Then $3 \leq d_2^\perp \leq 4$. Furthermore, in the special case of $p = 3$, let $c = (c_1, c_2, \dots, c_{n_2})$ be a codeword of $C_{D_2}^\perp$ with the minimum weight. Then $d_2^\perp = 4$ if there exist three nonzero components c_i, c_j, c_k of c such that $c_i = c_j = c_k = 1$ or 2, for some positive integers $i, j, k \in \{0, 1, \dots, n_2 - 1\}$. Otherwise, $d_2^\perp = 3$.

Proof. Clearly, $d_2^\perp \geq 2$. Now we could prove that $d_2^\perp \neq 2$. By the definition of C_{D_2} , $d_2^\perp = 2$ if and only if there are two distinct elements $x_1, x_2 \in F_{p^{2m}}^*$ and $c_1, c_2 \in F_p^*$ such that

$$\begin{aligned} c_1(Tr_1^m(\gamma x_1^{p^m+1}) + Tr_1^s(\beta x_1)) + c_2(Tr_1^m(\gamma x_2^{p^m+1}) + Tr_1^s(\beta x_2)) \\ = Tr_1^m(\gamma(c_1 x_1^{p^m+1} + c_2 x_2^{p^m+1}) + \beta^{p^m}(c_1 x_1^{p^m} + c_2 x_2^{p^m}) + \\ \beta(c_1 x_1 + c_2 x_2)) = 0. \end{aligned}$$

for all $\gamma \in F_{p^m}$ and $\beta \in F_q$. This is equivalent to

$$\begin{cases} c_1 x_1^{p^m+1} + c_2 x_2^{p^m+1} = 0, \\ c_1 x_1^{p^m} + c_2 x_2^{p^m} = 0, \\ c_1 x_1 + c_2 x_2 = 0. \end{cases} \quad (6)$$

By the equations of (6), we have

$$c_1 \frac{c_2^2}{c_1^2} x_2^{p^m+1} + c_2 x_2^{p^m+1} = \frac{(c_2^2 + c_1 c_2) x_2^{p^m+1}}{c_1} = 0.$$

Therefore, we have $c_2 = 0$ or $c_2 = -c_1$, which is a contradiction to the facts that $c_2 \in F_p^*$ and $x_1 \neq x_2$, respectively.

As the minimum weight of any linear code with length $p^{2m} - 1$ and dimension $3m$ is at most 4 due to the Sphere Packing Bound, we have $d_2^\perp \leq 4$. This completes the proof of the conclusion in the first part of this theorem.

Now we consider the special case that $p = 3$. Obviously, $C_{D_2}^\perp$ has a codeword of weight three if and only if there are three pairwise distinct elements $x_1, x_2, x_3 \in F_{3^{2m}}^*$ and three elements $c_1, c_2, c_3 \in F_3^*$ such that

$$Tr_1^m(\gamma(c_1x_1^{3^m+1} + c_2x_2^{3^m+1} + c_3x_3^{3^m+1}) + \beta^{3^m}(c_1x_1^{3^m} + c_2x_2^{3^m} + c_3x_3^{3^m})) + \beta(c_1x_1 + c_2x_2 + c_3x_3) = 0,$$

for all $\gamma \in F_{3^m}$ and $\beta \in F_{3^{2m}}$. This is equivalent to

$$\begin{cases} c_1x_1^{3^m+1} + c_2x_2^{3^m+1} + c_3x_3^{3^m+1} = 0, \\ c_1x_1^{3^m} + c_2x_2^{3^m} + c_3x_3^{3^m} = 0, \\ c_1x_1 + c_2x_2 + c_3x_3 = 0. \end{cases} \quad (7)$$

Without loss of generality, we only need to consider the following two subcases, since other situations are equivalent to the two subcases.

1. We assume that $c_1 = c_2 = c_3 = 1$ or $c_1 = c_2 = c_3 = 2$, which is the first case. It then follows from the last equations of (7) that $x_1 = -(x_2 + x_3)$. We have

$$\begin{aligned} (-x_2 - x_3)^{3^m+1} + x_2^{3^m+1} + x_3^{3^m+1} &= 2x_2^{3^m+1} + 2x_3^{3^m+1} \\ + x_2x_3^{3^m} + x_3x_2^{3^m} &= 2x_2^{3^m+1} + 2x_3^{3^m+1} - 2x_2x_3^{3^m} - 2x_3x_2^{3^m} \\ &= 2(x_2 - x_3)^{3^m+1} = 0, \end{aligned}$$

which is a contradiction. When $c_1 = c_2 = c_3 = 2$, the proof of this case is similar to $c_1 = c_2 = c_3 = 1$.

2. $c_1 = c_2 = 1, c_3 = -1$, other cases are similar to it. From the last equations (7), we have $x_3 = x_1 + x_2$ and

$$\begin{aligned} -(x_1 + x_2)^{3^m+1} + x_1^{3^m+1} + x_2^{3^m+1} &= -x_1x_2^{3^m} - x_1x_2^{3^m} = \\ x_1x_2(x_1^{3^m-1} + x_2^{3^m-1}) &= 0. \end{aligned}$$

Clearly, it is possible that $(\frac{x_2}{x_1})^{3^m-1} = -1$. Therefore, the proof of this theorem is now completed. \square

Example 4.3. Let $p = 5$ and $m = 1$. Then the code $C_{D_2}^\perp$ has parameters $[24, 21, 3]$ and is optimal.

Example 4.4. Let $p = 3$ and $m = 2$, the code $C_{D_2}^\perp$ has parameters $[80, 74, 3]$ and is optimal.

V. CONCLUSION

In this paper, we generalized the construction of linear codes by Ding et al[3]. The general construction method can get linear codes with flexible lengths and dimensions. Besides, linear codes over F_p have wide applications which are used for the construction of secret sharing schemes[3] and authentication codes[15]. Let w_{min} and w_{max} denote the minimum and maximum nonzero Hamming weights of the code C . In order to obtain secret sharing with interesting access structures, we would like to have linear codes C such that $\frac{w_{min}}{w_{max}} > \frac{p-1}{p}$ [16].

Then for the code C_{D_1} and C_{D_2} of Theorem 2.1 and 2.3 we have

$$\frac{w_{min}}{w_{max}} = \frac{(p^{2m-e-1} - p^{m-1})(p-1)}{p^{2m-e} - p^{2m-e-1}} > \frac{p-1}{p}.$$

$$\frac{w_{min}}{w_{max}} = \frac{p^{2m-1}(p-1) - p^{m-1}}{(p^{2m-1} + p^{m-1})(p-1)} > \frac{p-1}{p}.$$

Hence, the linear codes C_{D_1} and C_{D_2} of this paper satisfy the condition that $\frac{w_{min}}{w_{max}} > \frac{p-1}{p}$ and can be employed to obtain secret sharing schemes with interesting access structures using the framework in [16].

REFERENCES

- [1] C. Carlet, C. Ding and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 2089-2102, Jun. 2005.
- [2] J. Yuan, C. Carlet and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 712-716, Feb. 2006.
- [3] K. Ding and C. Ding, "Binary linear codes with three weights," IEEE Trans. Inf. Theory, vol. 18, no. 11, pp. 1879-1882, Nov. 2014.
- [4] K. Ding and C. Ding, "A class of two-weight and three-weight codes and their applications in secret sharing," IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 5835-5842, Nov. 2015.
- [5] Q. Wang, K. Ding and R. Xue, "Binary linear codes with two weights," IEEE Trans. Inf. Theory, vol. 19, no. 7, pp. 1097-1100, Jul. 2015.
- [6] Y. Qi, C. Tang and D. Huang, "Binary linear codes with few weights," IEEE Commun. Lett., vol. 20, no. 2, pp. 208-211, Feb. 2016.
- [7] C. Ding, J. Luo, and H. Niederreiter, "Two weight codes punctured from irreducible cyclic codes," in Proc. 1st Int. Workshop coding Theory Cryptogr., 2008, pp. 119-124.
- [8] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," Finite Fields Appl., 14 (2008) 390-409.
- [9] Z. Heng and Q. Yue, "A class of binary linear codes with at most three weights," IEEE Commun. Lett., vol. 19, no. 9, pp. 1488-1491, Sep. 2015.
- [10] C. Tang, N. Li, Y. Qi, Z. Zhou and T. Hellesteth, "Two-weight and three-weight linear codes from weakly regular bent function," arXiv:1507.0148v3.
- [11] W. C. Huffman and V. Pless, "Fundamentals of Error-Correcting Codes," Cambridge, U.K.: Cambridge Univ. Press, 2003.
- [12] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," Finite Fields Appl., 14 (2008) 390-409.
- [13] X. Zeng, L. Hu, W. Jiang, Q. Yue and X. Cao, "The weight distribution of a class of p-ary cyclic codes," Finite Fields Appl., 16 (2010) 56-73.
- [14] C. Ding, J. Yang, "Hamming weight in irreducible cyclic codes," Discrete Math., 313 (4) (2013) 434-446.
- [15] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," Theoretical Comput. Sci., vol. 330, no. 1, pp. 81-99, Jan. 2005.
- [16] J. Yuan and C. Ding, "Secret sharing schemes from two-weight codes," in Pro. R.C. Bose Centenary Symp., Discr. Math. Appl., Kolkata, India, Dec. 2002, p. 232.
- [17] C. Li and Q. Yue, "Weight distributions of cyclic codes with respect to pairwise coprime order elements," Finite Fields Appl., vol.28, pp. 94-114, Jul. 2014.
- [18] T. Hellesteth and A. Kholosha, "Monomial and quadratic Bent functions over the finite fields of odd characteristic," IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 2018-2032, May. 2006.